Available online at www.elixirpublishers.com (Elixir International Journal)

International Law

Elixir Inter. Law 118 (2018) 50642-50645

ISSN: 2229-712X

Cybercrime and the Law: A Review of the Kenyan Laws on Cybercrime.

Jackson Bett
Department of Commercial Law, School of Law, University of Nairobi, Kenya.

ARTICLE INFO

Article history:
Received: 21 March 2018;
Received in revised form:
24 April 2018;
Accepted: 5 May 2018;

Keywords
Cybercrime,
Cybersecurity
Cyber laws,
Enforcement.

ABSTRACT

The past half-decade has witnessed exponential use of the social media in Kenya. This has been made possible through enhanced internet connectivity especially through the use of mobile phones. Cybercrime has therefore emerged as a serious threat. Surprisingly, cybercriminals appear undeterred by the prospect of arrest and prosecution as they operate with impunity on the internet posing a risk to the financial health of corporations, privacy of the citizens who use the internet and also posing a threat to the security of the nation. The media has reported numerous occasions when cybercriminals have managed to interfere with the operations of the state. The alleged interference of Russian hackers in the 2016 US presidential election demonstrated how cybercriminals posed a threat to democratic institutions and democratic processes. Similar allegations were made in relation to the2013 and 2017 presidential elections in Kenya. It has also been reported that the terrorist group, ISIS (Islamic State of Syria and Iraq) has unit of hackers known as the Cyber Caliphate whose primary function is to propagate the ISIS agenda online. Most recently, the members of parliament in Kenya called upon the Inspector General of the Police and mobile service providers to launch investigations into cons who are registering numbers in their names and sending obscene images. This paper will examine the laws governing cybercrime in Kenya and make suggestions on law review to deal with the cybercrime menace.

Introduction

Cybercrime is an offence that is committed with the use of computer as a tool or as the target victims. The Kenya Information and Communications Act 2013 defines *cybersecurity as the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches used to protect the cyber environment.* The widespread adoption of computer and mobile technology in Kenya has led the rise of a new class of crimes that occur in the cyberspace such as hacking, email phishing and social engineering and Distributed Denial of Service (DDoS). For the last 7 years, Kenya has experienced a drastic increase in the number of reported cybercrimes. The financial services sector has suffered the heaviest damage as a result of cybercrime attacks. The Serianu Cybersecurity Report of 2016 revealed that the financial services sector lost over Ksh. 17 billion as a result of cybercrime. Financial institutions are the prime target for cybercriminals and crypto-anarchists.[1] The Kenya Revenue Authority (KRA) has also suffered major losses as a result of cybercrime. In March 2017, a man was arrested for allegedly hacking the KRA servers after which

KRA occasioned a Ksh. 4 billion losses.[2] Cybercrime has become the second most financially damaging crime in Kenya after corruption and economic crimes.

Despite the heavy losses occasioned by financial institutions, little focus and attention is given to the scourge of cybercrimes in Kenya. Financial institutions opt to keep the information about their losses private and incur the loss internally due to the fear of the negative publicity. Cybercriminals and crypto-anarchists have also targeted at the heart of our democratic processes and progress. The 2013 and 2017 General Elections in Kenya were marred with hacking claims.[3] Improper conduct of the IEBC during the relay and the transmission of presidential results in Kenya formed the basis for the nullification of the presidential election results in 2017 by the supreme court.

Despite the heavy losses occasioned by Kenya as a result of cybercrime, our democratic processes and financial institutions often find themselves helpless in the face of these attacks. Cybercrime is not a problem that is unique to Kenya but there is a need to curb the lawlessness in the Kenyan cyberspace. Financial and democratic processes are usually advised to follow the self-protection principle in preventing invasive cybercrime attacks. The cross-jurisdictional nature of cybercrime makes it difficult for offenders to be caught and brought to justice.

[1]SERIANU (2017). Africa Cybersecurity Report 2016. Nairobi: Paladion, pp.1-72.
[2]Maureen Kakah, 'Hacker To Remain In Custody In Sh4bn KRA Theft Case' (*Daily Nation*, 2017) <http://www.nation.co.ke/news/Alex-Mutungi-Mutuku-KRA-cybercrime-kenya/1056-3867562-10bq6hvz/index.html> accessed 11 Sept 2017.
[3]Wambua, S. (2017). Election 2017: Raila Odinga says IEBC database hacked and results altered. [online] The Standard. Availableat:https://www.standardmedia.co.ke/article/2001250797/election-2017-raila-odinga-says-iebc-database-hacked-and-results-altered [Accessed 18 Sep. 2017].

Tele:
E-mail address: jbett@uonbi.ac.ke

The architecture of the internet allows cybercrime offenders to operate anonymously without being traced. This paper will examine the laws governing cybercrime in Kenya and make suggestions on the most appropriate reforms.

Kenya Information and Communications Act 2013

This is the principal legislation governing the conduct of individuals and institutions with regard to e-commerce and electronic transactions. The security of electronic transactions and e-commerce is discussed in detail in Section VI of the Act. This section recognizes the validity of electronic signatures in verifying electronic transactions. Section 85S gives authority for the government and its agencies to use electronic signatures to facilitate service delivery. Electronic signatures, however, do not apply in the creation or the execution of a will, the documents of title and formation of negotiable instruments. Section 83U states that any person who causes a computer to perform a function knowing that the access he has secured is unauthorized, shall commit an offence and shall upon conviction be liable to fine not exceeding two hundred thousand shillings, or imprisonment for a term not exceeding two years or both. However, the person will not be liable when it is proved that the person had the right of control, was acting in good faith, there was express or implied permission of the owner of the computer systems to have such access, there are grounds to believe there are reasonable consent and the person was acting in pursuant to a statutory power. Section 83W deals with unauthorized access with the intent to commit an offence and gives same punishment as outlined in section 83U upon a successful conviction. Section 83W (4) further states that it does not matter whether the access was directed to another program, computer system or data held within a computer system, the offence shall be deemed to have been committed. Section 83X states that any person who knowingly causes the modification of a computer system upon conviction shall be liable to a fine not exceeding five hundred thousand, a jail term of three years or both.

The right to privacy for internet users in Kenya is further protected under 83Z where any person who knowingly discloses passwords, access codes or any other means of gaining access to data stored in a computer program for unlawful use, wrongful gain or knowingly that the computer will cause prejudice to a person shall be deemed to have committed an offence.

Section 84A of the act prohibits the trade and distribution of hacking tools. It states that any person who knowingly manufactures, sells, procures for use, imports, distributes or otherwise makes available a computer system or any other device designed or adapted primarily for the purpose of committing any offence under sections 83U to 83Z, shall commit an offence. Section 84A (3) further states that any person who receives or is found in possession of computer program or software with the intention of that data being used to commit a crime shall commit an offence.

Property rights in the cyberspace are protected by article 84B which states that any person who causes loss of property to a person by input, deletion or suppression of data or the interference with the functioning of a computer with the intent to procure himself or another person shall commit an offence and shall, on conviction be liable to a fine not exceeding two hundred thousand shillings and or imprisonment for a term not exceeding three years or both.

The fine for attempting or securing unauthorized access to protected system is one million.

Other offences mentioned in this section are the publication of obscene material, forging an electronic signature and reprogramming of a mobile phone device without express permission from the manufacturer. Reprogramming mobile phone devices without the permission of the manufacturer carries the heaviest penalty of one million, a prison term of five years or both.

Section 29 of the Kenya Information and Communication Act was ruled to be unconstitutional in Petition 149 of 2015.[4] Section 29 criminalizes sending message or other matter that is grossly offensive or of an indecent, obscene or menacing character. Justice Mumbi Ngugi ruled that the section was too broad and vague. It also violated the freedom of expression and article 50(2) of the constitution which provides the right to a fair trial.

Section VI of the Kenya Information and Communications Act has gained little traction in Kenyan courts because of the low conviction rates among offenders. Cybercrimes tend to be cross-jurisdictional and as such it is difficult to launch a successful conviction.[5] The evidential burden of proof is on the prosecution and they have to demonstrate that the accused was in control of the device or computer used for carrying out the attack when the offence was committed.

Anti-Corruption and Economic Crimes Act 2003

This act primarily deals with the protection of public revenue and public property. The act also protects public property and revenue from cybercrime. Section 45(c) states that A person is guilty of an offence if the person fraudulently or otherwise unlawfully damages public property, including causing a computer or any other electronic machinery to perform any function that directly or indirectly results in a loss or adversely affects any public revenue or service. This Act protects bodies that are charged with the responsibility of collecting and distributing public funds. Hackers have begun targeting KRA, NTSA and Kenya Power leading to monumental losses in pubic revenue.

The public bodies face a unique challenge because most of the cyber-attacks are not carried out from the country but from foreign nations. Cybercriminals attacking Kenyan bodies are stationed in countries that do not have an extradition treaty with Kenya. Prosecuting these offenders would require international collaboration between countries and by that time the offenders are extradited if Kenyan officials are able to do so, the evidence would have been destroyed.

Evidence Act

Part VII of the Evidence Act gives the procedures and guidelines which should be followed in admitting electronic records into evidence. Section 106B recognizes information contained in electronic records to be documents and as such they are admissible into evidence in relation to the Act. For electronic records to be admitted into evidence, there are multiple conditions that must be met. Section 106 B (2) list the four conditions that must be met when reviewing electronic evidence. The first condition that must be met is

[4]Geoffrey Andare v Attorney General & 2 others [2016] eKLR.

[5]O'Connor, V. (2012, March). Common Law and Civil Law Traditions. International Network to Promote the Rule of Law. Retrieved on 8th September 2017 from http://inprol.org/sites/default/files/publications/2012/common_law_civil_law_pg_fin al.pdf.

that the computer output was produced during the ordinary course of business and the person producing it had lawful control over the computer. The second condition was that the information was regularly fed into the computer during the ordinary course of business. The third condition that must be met was that the computer was operating properly and if not the period when the computer was not operating properly it must be demonstrated that the integrity of the electronic records was not compromised. The final condition is that the information contained in the electronic evidence reproduces or was fed in the ordinary course of business when the said activities happened.

Section 106B places a very high evidential burden on the prosecution because it is difficult to prove that the accused was the only one with the control of the computer or computer systems. The majority of the attacks span for weeks and during this time both the attacker and the system user explores the weaknesses of the system. By the use of keystroke logger, confidential information is stolen from the system. The attacker may also modify electronic records and therefore compromise the integrity of the computer systems.

Section 106B (4) states that electronic records must be accompanied by a certificate in order for the evidence to be admissible. Electronic evidence without the accompanying certificate has little or no probative value. It is paramount to note that before cybercrime investigators conduct their search they must comply with the governing laws of criminal and civil procedure. Any data that was obtained without search warrant is not admissible as electronic evidence. There are four exceptions where cybercrime investigators can conduct a search and collect electronic evidence without a search warrant. These exceptions are national emergency, consent or under the plain view doctrine.

The Penal Code

Section 357 (b) of the Penal Code states that any person, who with the intent to defraud or deceive knowingly utters any document or electronic record or writing so made, signed or executed by another person, is guilty of a felony and is liable to imprisonment for seven years. This section is applicable to incidences of forgery of electronic documents or electronic signatures in order to commit a crime.

Section 348 of the penal code states that an intent to defraud is presumed to exist if it appears that at the time when the false document was made there was in existence a specific person ascertained or unascertained capable of being defrauded thereby. The intent to defraud further states that the presumption of the intent to defraud is not rebutted by the fact that the offender took steps to prevent the victim from being defrauded or that the offender thought that he had a right to the thing that he sought with false document.

Section 348 and 357(b) of the penal code largely deals with preventing identity theft in order to commit a cybercrime. The theft of digital identity the avenue through which most of the fraud and forgery incidences that take place online. Kenya does not have a law to protect the online identities of its citizens. Without a proper framework to protect internet users, confidential information is often used get improper access to government services online through e-citizen platform.

The Sexual Offences Act (2006)

Despite the concerted international effort to curb child pornography, the industry has continued to thrive in the dark web. Images of children taking part in child pornography are still distributed across the internet with the aid of obfuscation and encryption. Section 16 of the Sexual Offences Act prohibits the making, sale, advertisement, distribution or profiting from child pornography. Any person who is found guilty is liable for an imprisonment of not less than 6 years and a fine not less than five hundred thousand. Upon a subsequent conviction, the person will be liable for imprisonment of a prison term of seven years without the option of a fine.

Section 16 of the act does not apply where the drawing or publication can be justified on the ground of public good on the ground that such publication or drawing is in the interest of science, ancient religion, learning, literature and other objects of general concern.

National Intelligence Service Act

Section 5(1) q states that one of the functions of the National Intelligence Service is to provide material support, advice and assistance to state officers, state organs and state departments on matters relating to the security and the integrity of information that is stored and processed in electronic means. According to this section, the National Intelligence Service is responsible for combing through the ICT infrastructure used by the state and identifying the potential weaknesses and vulnerabilities that place the country at risk.

The rise of cybercrime black market, where information stolen from state agencies is traded for profit has put western countries on high alert. The National Intelligence Service should carry out this function effectively to ensure that the critical ICT infrastructure of the country does not come under attack and jeopardize national security.

Copyright Act

Digital piracy is the illegal trade and distribution of copyrighted software, videos and digital video devices. The digital piracy takes place when someone other than the copyrighted owner copies the product and sells it for a portion of the price sold by the copyright holder.[6] Before the advent of the internet it was easy for copyright laws to be enforced in print and electronic media. The internet allows copyrighted works to be distributed across file sharing sites on the internet. Electronic rights management has become difficult for content producers.

The Copyright Act of Kenya defines electronic rights management as any information by rights holders which identifies the work or recording. Section 35(3) of the copyright Act states that copyright shall be infringed by a person who, circumvents any effective technical measure designed to protect works, removes or alters any electronic rights management information; or (d) distributes, imports, broadcasts or makes available to the public, protected works, records or copies from which electronic rights management information has been removed or has been altered without the authority of the right holder.

Peer to peer distribution of copyrighted files, illegal download of copyrighted music and videos and download of pirated software are the most common cybercrimes. These activities are so common and are carried out in large scale.[7]

[6]Ben Sihanya (2005; published 2006) "Copyright law, teaching and research in Kenya," East African Law Journal Vol 2 2005 at pp. 28-62.

[7]Dr. Mihaly Fiscor (2002) Collective Management of Copyright and Related Rights, World Intellectual Property Organisation, Geneva.

Digital piracy is seen as a victimless crime and developing countries such as Kenya have limited resources to enforce copyright laws.Strict enforcement of copyright laws is seen as a hindrance to growth and innovation.

Computer and Cybercrime Bill 2016

The Computer and Cybercrime Bill of 2016 is a proposed legislation that will seal the legal loopholes and give the country a comprehensive legislation on handling cybercrime. Cybercriminals and crypto-anarchists have repeated targeted government ICT infrastructure. The bill provides for a protected computer, a term that was missing in the Kenyan legal terminology. Section 9(2) of the bill defines a protected computer as a computer system that is used directly in connection with a) security, defense, and international relations, b) existence or the identity of confidential source of information relating to the enforcement of criminal law c) the provision of services directly related to communications infrastructure, banking and financial services, payment and settlement systems and instruments, public utilities or public transportation, including government services delivered electronically; d) the protection of public systems relating to public transportation, medical services, emergency systems with the police and the provision of national registration systems. The offences involving a protected computer system carry a fine not exceeding 25 million or a prison term not exceeding 20 years or both. The bill increases the fine for child pornography offences to 25 million and a prison term not exceeding 20 years from the current prison sentence of 7 years. The computer and Cybercrime Bill 2016 provides for a new class of crimes that are missing in the current legal framework on cybercrime such as cyberstalking and provides a framework for international collaboration in order to solve cybercriminal activities.

Conclusion

The availability of high speed internet has allowed millions of Kenyans to be connected to the internet. The internet has created a new class of crimes that are difficult to detect and prosecute. Cybercriminals and crypto-anarchists operate in the Kenyan cyberspace with impunity. The existence of the tor browser and tails operating system have made it difficult for cybercriminals to be detected. The cross-jurisdictional nature of cybercrime makes it difficult for cybercrime investigators in Kenya to investigate and bring those responsible to justice. There is a need for broader international co-operation in order to curb cybercrime. The Parliament should pass the Computer and Cybercrime Bill of 2016 in order to make Kenya to be adequately prepared to handle the unique challenges posed by cybercrime to our economy and to our national security.

Bibliography

Cases

Geoffrey Andare v Attorney General & 2 others [2016] eKLR.

Legislations

1. Kenya Information and Communications Act 2013.
2. Anti-Corruption and Economic Crimes Act 2003.
3. Evidence Act.
4. Sexual Offences Act 2006
5. The Penal Code
6. The National Intelligence Service Act
7. The Copyright Act
8. Proposed Legislation
9. Computer and Cybercrimes Bill 2016

Reports

1. SERIANU (2017). Africa Cybersecurity Report 2016. Nairobi: Paladion, pp.1-72.
2. Dr Mihaly Fiscor (2002) Collective Management of Copyright and Related Rights, World Intellectual Property Organisation, Geneva.

Journal Article

Ben Sihanya (2005; published 2006) “Copyright law, teaching and research in Kenya,” East African Law Journal Vol 2 2005 at pp. 28-62.

Articles in a periodical

1. Maureen Kakah, 'Hacker to Remain In Custody In Sh4bn KRA Theft Case' (*Daily Nation*, 2017)<http://www.nation.co.ke/news/Alex-Mutungi-Mutuku-KRA-cybercrime-kenya/1056-3867562-10bq6hvz/index.html> accessed 11 Sept 2017.
2. Wambua, S. (2017). Election 2017: Raila Odinga says IEBC database hacked and results altered. [online] The Standard.Availableat:https://www.standardmedia.co.ke/article/2001250797/election-2017-raila-odinga-says-iebc-database-hacked-and-results-altered, accessed 18 Sep. 2017.
3. O’Connor, V. (2012, March). Common Law and Civil Law Traditions. International Network to Promote the Rule of Law. Retrieved on 8th September 2017 from http://inprol.org/sites/default/files/publications/2012/common_law_civil_law_pg_fin al.pdf.